# 物联网安全需求及对策

创新中心 张星

关键词：物联网安全需求 物联网需求 物联网需求分析

摘要：物联网很多应用都与日常生活息息相关，一些不恰当的方案设计，可能会直接或间接地暴露用户的隐私信息，了解物联网所面临的安全威胁并找到制定对策的方法是非常重要的。本文是物联网安全系列文章的第二篇，接续上期物联网安全概述之后，讨论《物联网安全的需求与对策》

## 一．引言

物联网技术的出现，使我们的生活更加方便、快捷的同时，也不可避免地带来了一些安全问题。物联网中的很多应用都与我们的生活息息相关，如摄像头，智能恒温器等设备，通过对它们的信息的采集，可直接或间接地暴露用户的隐私信息。由于生产商缺乏安全意识，很多设备缺乏加密、认证、访问控制管理的安全措施，使得物联网中的数据很容易被窃取或非法访问，造成数据泄露。物联

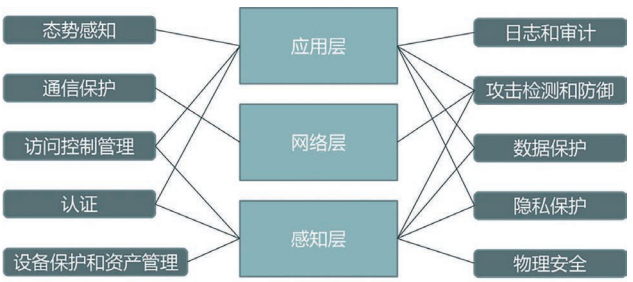



图 2.1 物联网各层的安全需求

网这种新型的信息网络往往会遭受有组织的 APT 攻击。由此可见，物联网安全问题需要引起我们的高度重视。

物联网涵盖范围广泛，本章关注于物联网安全中较为通用的安全需求，并给出了相应的对策，让读者对物联网安全需求和研究方向有更加深刻的了解。通过图 2.1，也可以发现，物联网的不同层次可能面临相同的安全需求。

## 二．物联网威胁与对策

### 2.1 隐私保护

物联网中的很多应用都与我们的生活息息相关，如摄像头，智能恒温器等设备，通过对它们的信息的采集，会直接或间接地暴露用户的隐私信息。所以隐私保护是物联网安全问题中应当注意的问题之一。

（1）威胁

基于数据的隐私威胁：物联网中数据采集、传输和处理等过程中的隐私信息泄露。

基于位置的隐私威胁：物联网中各节点的位置隐私以及物联网在提供各种位置服务时的位置隐私泄露问题。

（2）对策

通信加密。

最小化数据采集。

匿名化数据采集和处理。

由相关用户决定是否授权数据采集。

路由协议隐私保护法保护节点准确位置信息。

### 2.2 认证

（1）威胁：

物联网环境中的部分访问无认证或认证采用默认密码、弱密码。

（2）对策：

一方面开发人员应考虑在设计时确保用户在首次使用系统时修改默认密码，尽可能使用双因素认证，对于敏感功能，需要再次进行认证等；

另一方面作为用户，应该提高安全意识，采用强密码并定期修改密码。

### 2.3 访问控制管理

（1）威胁：

未授权访问

安全配置长期不更新、不核查

（2）对策：

身份和访问管理、边界安全（安全访问网关）。

持续的脆弱性和错误配置检测清除。

网关是很多公司的关注点。Vidder 公司的产品基于 CSA 定义的软件定义边界，只有认证后才能对服务进行访问。CUJO 公司的智能防火墙，采用了网关 + 云 + 手机 APP 的模式，手机 APP 可以看到对于内部网络的访问情况，并进行访问控制，云端对网关采集的流量数据进行分析并提供预警。

未来的智能家庭安全将会是一个关注点，随着家庭中智能设备的增多，设备本身的访问控制并不足以抵抗日益复杂的网络攻击，如果设备本身存在漏洞，攻击者将可能绕过设备的认证环节。一个自然的思路是在网络的入口做统一的访问控制，只有认证的流量才能够访问内部的智能设备。

### 2.4 数据保护

（1）威胁：

数据的泄露和篡改问题。如基于修改的医疗数据，医疗服务提供者有可能错误地对患者进行诊断和治疗。

（2）对策：

很多公司都提供了 DLP 产品。

对于物联网环境下的数据安全问题，信息安全公司一般采用将已有的 DLP 产品作为解决方案的一部分进行推出。

### 2.5 物理安全

（1）威胁：

部署在远端的缺乏物理安全控制的物联网资产有可能被盗窃或破坏。

（2）对策：

尽可能加入已有的物理安全防护措施。

并非技术层面的问题，更应作为标准的一部分进行规范。

### 2.6 设备保护和资产管理

（1）威胁：

设备的配置文件被修改。

设备的数量巨大使得常规的更新和维护操作面临挑战。

未认证代码执行。

断电引发的异常。

设备逆向工程。

（2）对策：

定期审查配置。

固件自动升级（over-the air（OTA））。

定义对于物联网设备的全生命周期控制。

对代码签名以确保所有运行的代码都是经过认证的，以及在运行时防护。

断电保护。

用白盒密码来应对逆向工程。

物联网环境下有两点尤其要注意，一是众多设备如何升级，二是对于设备的逆向工程。对于第一点，应定义对于物联网设备的全生命周期控制，并提供设备固件自动升级的方式；对于第二点，目前已知的技术是采用白盒密码。

### 2.7 攻击检测和防御

拒绝服务攻击

（1）威胁

在物联网中拒绝服务攻击主要分为两种，一种是对设备进行攻击，如：一直给电子标签发送恶意请求信息，使标签无法响应合法

请求，另一种是控制很多物联网设备对其它系统进行攻击。

（2）对策

针对第一种攻击，物联网远端设备需要嵌入式系统抵抗拒绝服务攻击。针对第二种攻击，一方面加强对节点的保护，防止节点被劫持，另一方面也需要提供有效地识别被劫持的节点的方法。

Zilog 和 Icon Labs 联合推出了使用 8 位 MCU 的设备的安全解决方案。防火墙控制嵌入式系统处理的数据包，锁定非法登录尝试、拒绝服务攻击、packet floods、端口扫描和其他常见的网络威胁。

病毒攻击

（1）威胁

病毒攻击指在计算机程序中插入的破坏计算机功能或者数据的代码。

（2）措施

物联网设备需要代码签名，以确保所有运行的代码都是经过授权和认证的。

赛门铁克的白皮书中指出设备保护需要对代码签名以确保所有运行的代码都是经过认证的；天威诚信 VeriSign 代码签名证书；Instant SSL、微软、Digicert 等都在做代码签名相关的工作。

APT 攻击

（1）威胁

APT（Advanced Persistent Threat）指的是高级持续性威胁。利用先进的攻击手段有组织地对特定目标进行长期持续性网络攻击。APT 入侵途径主要包括以下几个方面。

（1）以智能手机、平板电脑和 USB 等移动设备为攻击对象，进而入侵企业信息系统。

（2）恶意邮件，钓鱼网站，恶意链接等。

（3）利用防火墙、服务器等系统漏洞继而入侵企业网络。

（2）对策

（1）使用威胁情报。

及时获取最新的威胁情报信息，如：APT 操作者的最新信息；不良域名；恶意邮件地址，附件，主题；恶意链接和网站等信息，及时进行防护。

（2）建立防火墙和网关，进行访问控制。定期检查配置信息，及时更新升级。

（3）收集日志进行分析和溯源。

（4）全网流量行为的模型建立和分析。

（5）对用户的访问习惯进行监测。

在检测到 APT 攻击的同时，也可以对 APT 攻击进行监测和溯源分析，并将威胁情报共享。

蜜罐

蜜罐是设置好故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的，可以让人随时了解针对系统所发动的最新的攻击和漏洞。

### 2.8 态势感知

态势感知是在大规模系统环境中，对能够引起系统状态发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。

这里我们将对一个态势感知系统中比较重要的几部分进行介绍。

异常行为检测

异常行为检测的方法一般是运用大数据分析技术，在特定的环境中，如工控领域等可以进行全流量分析和深度包检测。

一个异常行为检测系统应能自动进行异常行为检测，对客户的网络进行分析，知道什么是正常的行为，并建立一个基线，然后如果发现不正常的或者可疑的行为就会报警。除监视应用程序的行为外，它还应监视文件，设置，事件和日志，并报告异常行为。

总结来说有两种方法，一个是建立正常行为的基线，从而发现异常行为，另一种是对日志文件进行总结分析，发现异常行为。

脆弱性评估

客户如何知道他们是否采用了足够的安全措施，或者是否采用了正确的步骤来保护他们的资产和业务。客户需要从众多的公布的标准和最佳实践中获取信息来指导他们的工作，但是有时候阅读和理解一些相关的标准有些困难。所以需要为用户提供一套解决方案来被动或者主动地评估系统、网络和应用，发现不良行为，并不断提供脆弱性评估报告。

脆弱性评估应具备从多传感器中收集到的网络通信和事件信息数据来分析环境的脆弱性和威胁的能力，对 IT 安全进行持久的监控。

威胁情报交换

物联网设备的经销商、制造商甚至政府机构能够合作起来，及时发现各类木马病毒和 0day 漏洞威胁，防范并拦截 APT 攻击、未知威胁等新型恶意攻击，实现共赢局面。

Intel 白皮书中指出汽车的经销商、制造商甚至政府机构能够合作起来，进行威胁情报交换，能够快速将零日漏洞和恶意软件通知相应的车辆。CUJO 通过将流量信息与商业威胁情报源进行对比，以确保未授权的 IP 没有连接到用户的网络中。

通过利用威胁情报，及时对最新的攻击进行防御。当遭受到未知攻击的时候，及时将威胁情报发布出去，实现威胁情报的共享。

可视化展示

可视化展示能够直观的呈现数据特点，同时容易被读者接受和理解，所以大数据分析（深度包检测、全流量分析）结果需要可视化展示。

大多数分析系统都有可视化的功能，如：NexDefense 支持网络流量 3D 可视化等。

可以通过与手机 APP 结合实现移动可视化。

物联网事件响应措施

当系统遭到攻击时，需要快速的识别攻击来源，攻击路径，对攻击做出快速的响应，在攻击造成更大的破坏之前，实施有效的措施，减少损失。在攻击之后，需要快速地防止此类攻击的再次发生。

采用的策略一般是态势感知中的常用方法、异常行为检测和及时打补丁。

### 2.9 通信保护

物联网设备与设备之间，设备与远程系统之间需要进行通信，

如果通信缺少传输加密和完整性验证，那么通信很可能会被窃听或篡改。通信保护需要对于设备和远程系统之间的通信进行加密和认证。

很多公司的产品或者解决方案中都有数据的传输加密、以及授权和认证功能模块，如 Mocana 公司的安全服务平台；Arrayent 的 Arrayent Connect Platform；Device Authority 的 Data Centric Security Platform；SecureRF 开发了快速，超低功耗的加密工具，Bastille 指出的无线鼠标和键盘劫持问题也与通信保护有关。

在工控场景中，可通过单向网闸，实现数据只能从低安全等级的系统流向高安全等级的系统。

2.10 日志和审计

（1）威胁：

对于威胁的检测。

行业安全标准的合规。

（2）对策：

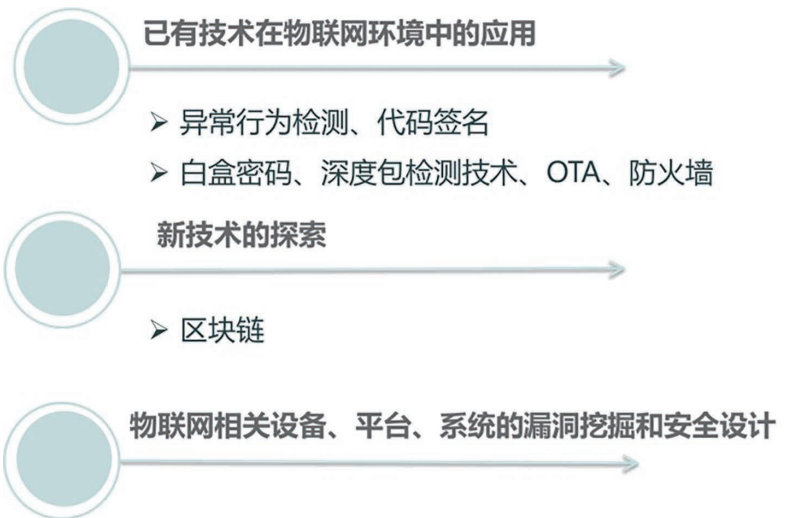
日志分析。

合规性检查。

从行业角度来说，特定行业的合规性必不可少。对于日志的分析有可能发现潜在的威胁，但关键点在大数据的分析能力。

**三．物联网安全技术**

物联网安全产品的核心在于技术，由于物联网的安全是互联网安全的延伸，那么我们可以利用互联网已有的安全技术，结合物联网安全问题的实际需要，改进已有技术，将改进后的技术应用到物联网中，从而解决物联网的安全问题。




通过对物联网安全需求和对策的分析，我们总结出需要重点关注的技术。后面我们将分别从已有技术在物联网环境中的应用、新技术的探索和物联网相关设备、平台、系统的漏洞挖掘和安全设计三个方面介绍物联网安全技术研究的一些思路。

在下一期文章中，我们接着讨论《物联网安全的相关技术》